



John Fouts <icreateupwardspirals@gmail.com>

2025-05-16 - Follow-Up on ASUS Security Case #N2411019565-0004 – Forensic Evidence Confirmed, National Complaints Filed - Re: 2025-05-12 - URGENT: ASUS Security Breach – Form Submission Blocked – Evidence Enclosed via Email

Wendy Vu (ACI) <wendy_vu@asus.com>

To: John Fouts <icreateupwardspirals@gmail.com>

Cc: Security <security@asus.com>, "Wendy Vu (ACI)" <wendy_vu@asus.com>

Hello Mr. Fouts,

Thank you for your detailed message and for your continued engagement regarding your concerns.

To ensure your submitted forensic evidence is fully received and properly reviewed by our internal team, we have had the necessary permissions enabled. Once uploaded, please provide the shareable link directly in your reply to this email.

This step is essential for us to move forward. Due to the technical limitations previously encountered by our IT and legal teams, we are now able to proceed with a thorough evaluation.

We appreciate your patience, cooperation, and understanding as we work to address your concerns.

Thank you, and we look forward to your reply.

Best regards,

Wendy Vu | Senior Supervisor of Customer Care

Service Department | Support Section | Corporate Customer Care

Phone: 510-739-3777 ext. 65008 | Email: Wendy_Vu@asus.com

ASUS Computer International | 48720 Kato Road, Fremont, CA 94538



From: John Fouts <icreateupwardspirals@gmail.com>

Sent: Friday, May 16, 2025 12:35 PM

To: Wendy Vu (ACI) <wendy_vu@asus.com>

Cc: Security <security@asus.com>

Subject: 2025-05-16 - Follow-Up on ASUS Security Case #N2411019565-0004 – Forensic Evidence Confirmed

External email : Ensure your email is secure before opening links and attachments.

To: Wendy Vu (Senior Supervisor, ASUS Corporate Care)

CC: ASUS Global Security Team, ASUS Legal Affairs, ASUS Executive Leadership

BCC: Legal Archive

Subject: Follow-Up on ASUS Security Case #N2411019565-0004 – Forensic Evidence Confirmed, National Complaints Filed

Dear Ms. Vu and the ASUS Global Security Team,

Thank you for your reply dated May 15, 2025, referencing case number N2411019565-0004.

Your message states that ASUS has “not found any confirmed vulnerabilities” but remains committed to a thorough review

1. Bulletproof Forensic Evidence Has Already Been Submitted

The materials I’ve already provided go beyond suspicion. They include:

- Firmware logs and ACPI dumps
- Network-level traces indicating unauthorized DNS redirection
- Persistent MAC spoofing and unexplained outbound traffic
- Evidence of virtualization/hypervisor intrusion
- Proof that all factory resets failed
- Affected devices: ASUS TUF A16, AX1800S, and AX5400 routers

This is not speculative. It is documented system compromise. If ASUS cannot identify a vulnerability from these artifacts, I

2. The security@asus.com Email Inbox Is Non-Functional

You instructed me to send documentation to security@asus.com. This address does not accept emails — I attempted to send

As of now, you have acknowledged the case but not acknowledged receipt of any attachments or confirmed internal delivery

3. National and Federal Oversight Bodies Have Been Contacted

This is no longer just an ASUS issue. My case is now active under multiple federal and state agencies, including:

- California Attorney General (privacy and consumer harm complaint)
- Federal Trade Commission (FTC) – cybersecurity negligence & consumer fraud
- California Privacy Protection Agency (CPPA) – CCPA violation complaint
- Cybersecurity & Infrastructure Security Agency (CISA) – active case: CCASE0086447
- Planned filings: FCC, IC3, and U.S. Secret Service Cybersecurity Division

I have also formally noted ASUS in active legal filings tied to whistleblower retaliation, unlawful surveillance, and digital surveillance

4. ASUS Must Escalate This to Legal and Executive Review

I now request, in no uncertain terms, that this matter be escalated to:

- Jonney Shih, S.Y. Hsu, Samson Hu, Joe Hsieh
- ASUS Legal and Regulatory Affairs
- An appropriate point of contact for coordination with federal investigative agencies

This is a high-risk cybersecurity matter with real-world medical and legal consequences, not a routine support ticket. I rem

5. Immediate Response Requested

Please provide, within 3 business days:

- Confirmation of which ASUS teams have reviewed the forensic materials
- A full audit trail of the internal investigation to date
- Official assurance that your systems for receiving security disclosures are being repaired

6. Unacceptable Delays and Unlawful Disregard of Critical Evidence

While your reply arrived on May 15, 2025, it followed several days of silence after I submitted urgent, well-documented, so deeply concerning.

Let me be direct: ASUS's failure to acknowledge or act upon the forensic-grade materials submitted is not only negligent –

The materials I shared are not theoretical or anecdotal. They represent:

- BIOS- and ACPI-level trace logs
- Network evidence of unauthorized DNS redirection and outbound traffic
- Persistent MAC spoofing
- Signs of firmware rewrite and hypervisor-based virtualization
- Continued breach behavior following factory resets

These are not abstract possibilities — they are empirical indicators of compromise, gathered using appropriate tools, unde

To dismiss or ignore these artifacts without transparent analysis and acknowledgment is not simply a communications failu

I am not asking for speculation or deference. I am requesting immediately:

1. Written confirmation that these materials were received, reviewed by qualified cybersecurity personnel and the nar
2. A complete audit trail of all investigative actions taken by ASUS since the case was opened with contact informatio
3. Immediate assignment of a named contact in both Global Security and Legal/Compliance to oversee this matter goi

Failure to provide these steps in a timely and complete manner will be noted in ongoing legal filings and federal agency co

If ASUS does not acknowledge receipt and act accordingly, this will be noted in pending filings with state and federal regul

To dismiss these findings without a transparent audit is not a customer service issue. It is a failure of legal compliance and

Statutory Violations Potentially Implicated

ASUS's current posture may constitute violations under the following:

- Federal Trade Commission Act (15 U.S.C. § 45) – for deceptive, unfair practices in commerce
- Computer Fraud and Abuse Act (18 U.S.C. § 1030) – for enabling access or failing to secure compromised systems
- Americans with Disabilities Act – Title III (42 U.S.C. § 12182) – for obstructing protected communication during AD/
- California Consumer Privacy Act (CCPA – Cal. Civ. Code § 1798.100)
- Cybersecurity Information Sharing Act (6 U.S.C. § 1501) – for failure to act on a legitimate security threat
- Whistleblower Protection under 18 U.S.C. § 1514A (SOX)
- Federal Communications Act (47 U.S.C. § 222 & § 605)

These statutes are not academic — they are active and enforceable, and this matter has already been submitted to:

- The California Attorney General
- The Federal Trade Commission (FTC)
- The California Privacy Protection Agency (CPPA)

- The Cybersecurity and Infrastructure Security Agency (CISA)
 - And will shortly be submitted to the FCC, the Secret Service Cybersecurity Division, and the IC3/NW3C
-

Immediate Required Actions from ASUS

1. Formally acknowledge that my submitted documentation was received and is being treated as a serious breach matter
2. Confirm internal escalation to both Global Security and Legal Divisions
3. Assign a named, direct contact from each team to correspond with me moving forward as asked for previously
4. Provide a full audit trail of internal actions taken since the case was first submitted

I am documenting this correspondence as part of multiple ongoing federal investigations and civil rights filings.

ASUS's continued failure to respond appropriately and in good faith will be cited accordingly.

I expect confirmation and a substantive response no later than Monday, May 20, 2025, by close of business.

Thank you again for your time. I look forward to your response.

Sincerely,

John R. Fouts, MBA

Federal Whistleblower | ADA-Protected Cybersecurity Survivor

E: icreateupwardspirals@gmail.com

P: 502.956.0052 (Text Only – ADA)

F: 502.996.8246 (HIPAA Compliant)

On Thu, May 15, 2025 at 6:26 PM Wendy Vu (ACI) <wendy_vu@asus.com> wrote:

Hello Mr. Fouts,

Thank you for staying in touch and for the detailed documentation you've provided so far.

After carefully reviewing the materials, we have not found any confirmed security vulnerabilities related to your report.

To ensure our Global Security Team has all the necessary information, please send any remaining documentation by the end of the week.

If you're having trouble uploading files, try breaking them into smaller parts or use a secure file-sharing service.

We appreciate your continued cooperation and thank you for bringing this to our attention. We take your concerns seriously.

Case Number: N2411019565-0004

Best regards,

Wendy Vu | Senior Supervisor of Customer Care

Service Department | Support Section | Corporate Customer Care

Phone: 510-739-3777 ext. 65008 | Email: Wendy_Vu@asus.com

ASUS Computer International | 48720 Kato Road, Fremont, CA 94538



From: John Fouts <icreateupwardspirals@gmail.com>

Sent: Sunday, May 11, 2025 11:11 AM

To: Security <security@asus.com>

Cc: Wendy Vu (ACI) <wendy_vu@asus.com>

Subject: 2025-05-12 - URGENT: ASUS Security Breach – Form Submission Blocked – Evidence Enclosed

External email : Ensure your email is secure before opening links and attachments.

Dear ASUS Security Advisory Team and Ms. Wendy Vu,

This is to notify you that I attempted to submit a formal report via the ASUS Security Advisory submission form, per your request. Unfortunately, the form is currently non-functional for real-world, urgent security disclosures.

This form is currently non-functional for real-world, urgent security disclosures. As a result, I am providing my report via email.

Case Summary

This is not a standard support matter. It is a **confirmed case of cybersecurity compromise, unlawful surveillance, and data breach.**

ASUS has already acknowledged the seriousness and gravity of these issues.

Immediate Actions Requested

1. **Confirm whether all prior documentation provided to Wendy Vu has been submitted internally to the ASUS Security Advisory Team.**
2. **Provide internal case reference ID, contact name, and the office handling ASUS' internal investigation.**
3. **Identify the ASUS point of contact for law enforcement coordination,** including the U.S. Secret Service Cyber Protection Center.
4. **Escalate immediately to ASUS Executive Leadership and Board of Directors,** including Jonney Shih, S.Y. Hsu, and other senior executives.

Attached / Enclosed Materials

Due to email size limits, I am sending only core attachments here. Additional evidence will be made available upon request.

- final_evidence_ocr_fixed.pdf
- ACPI Tables
- Gmail - 2025-05-07 - Subject_ Follow-Up on Escalated ASUS Security Case – Legal Notice
- Gmail - 2025-04-10 URGENT_ Cyber Espionage Report & Legal Notice – ADA-Protected
- Gmail - CISA Case_ CCASE0086447 Opened.pdf
- Gmail - [FCC Complaint] Hijacking, Firmware Rewrite, Digital Interference.pdf
- Other attached files

2025-03-29-IC3-Complaint-Submitted-For-Unusual-Malware-Found-On-Laptop-Steal

Cyber_Espionage_Legal_Notice_Meta.pdf

Gmail - [FCC Consumer Inquires and Complaints] Re_ FCC Urgent Complaint - Unlawful

Gmail - CISA Case_ CCASE0086447 Opened na.pdf

Gmail - Request received_ FCC Urgent Complaint - Unlawful Network Hijacking, Fir

If larger files or additional exhibits are needed, I can provide secure download links, file segments, or alternative transfer methods. I am willing to provide select critical forensic materials for internal review and coordination with appropriate investigative agencies. I am willing to provide select critical forensic materials for internal review and coordination with appropriate investigative agencies.

This is a matter of **grave urgency**. I remain under active threat. This is a matter of grave urgency, and I urge ASUS to take immediate action. I am willing to provide select critical forensic materials for internal review and coordination with appropriate investigative agencies.

John R. Fouts, MBA
Pro Se Whistleblower | Disabled Litigant

📞 Phone: 502-956-0052 (Text Only)
📠 Fax: 502-996-8246 (HIPAA Compliant)
✉ Email: icreateupwardspirals@gmail.com
📍 Current Location: Near Clifton, Louisville, KY

On Fri, May 9, 2025 at 1:07 PM Wendy Vu (ACI) <wendy_vu@asus.com> wrote:

Dear Mr. Fouts,

Thank you for your detailed message and for taking the time to provide further clarification regarding the information you've shared.

After careful review of the information you've shared, and consultation with several internal team members, we have forwarded your correspondence, documentation, and evidence to our dedicated security team. This team is best positioned to handle such matters and will provide a response as soon as possible. You can reach our security team at securityadvisory@asus.com.

For additional information about our security processes and how such cases are reviewed, please

- <https://www.asus.com/content/asus-product-security-advisory/>

We appreciate your cooperation in helping us ensure the integrity and security of our products, a

Best regards,

Wendy Vu | Senior Supervisor of Customer Care

Service Department | Support Section | Corporate Customer Care

Phone: 510-739-3777 ext. 65008 | Email: Wendy_Vu@asus.com

ASUS Computer International | 48720 Kato Road, Fremont, CA 94538



From: John Fouts <icreateupwardspirals@gmail.com>

Sent: Tuesday, May 6, 2025 9:39 PM

To: Wendy Vu (ACI) <wendy_vu@asus.com>

Cc: Jennifer Stover (ACI) <Jennifer_Stover@asus.com>; ic3@fbi.gov; consumer@ftc.gov; alerts@cisr.fbi.gov

Subject: 2025-05-07 - 12:08 a.m. - Subject: Follow-Up on Escalated ASUS Security Case – Legal and

External email : Ensure your email is secure before opening links and attachments.

Subject: Follow-Up on Escalated ASUS Security Case – Confirmed Device Compromise

Dear Ms. Vu,

Thank you for your response and for confirming escalation to ASUS Global Research and Development.

To clarify -- once more...

This is **NOT** a standard customer support case.

This matter involves **confirmed and reproducible evidence of device compromise** across multiple ASUS product

The issues documented are **not hypothetical or “potential.”**

They include:

- **Persistent firmware-level compromise** that survives factory reset
- **Remote access behaviors consistent with unauthorized control**
- **Manipulated traffic and DNS hijacking**, confirmed across clean networks
- **Hypervisor activity** not attributable to user configuration
- **Chain-of-custody and supply chain integrity failures**

These facts have been reported not only to ASUS, but also to **federal authorities**, including the:

FBI (IC3),

FTC, and

CISA,

due to the national cybersecurity implications of compromised infrastructure equipment.

I am prepared to provide the requested serial number in clearer form, of course.

However, I will not surrender these devices to ASUS without **neutral third-party forensic oversight or a federally s**

Further, **I strongly object to ASUS dismissing my other claims—such as damages and systemic negligence—**

They are **civil, criminal, and constitutional violations**, some of which may ultimately very likely involve ASUS

ASUS's formal participation may indeed be compelled by court order, and I reserve all rights to pursue that a

I expect immediate acknowledgment of:

1. ASUS's willingness to coordinate secure, traceable transfer of these devices for forensic analysis,
2. ASUS must provide **temporary replacement devices of equivalent functionality** for the duration of the inve
3. Your investigation timeline and scope, and
4. The name of the internal team lead for this case, all team members, and supervisory contacts.

To further support these issues, I have attached a compiled document that includes:

- **Clear and verifiable serial number identification**
- **Forensic logs and system data** indicating persistent compromise
- **Hardware-level output** that demonstrates unauthorized firmware behavior and security violations

Please confirm receipt and advise on next steps immediately.

Sincerely,

John R. Fouts, MBA

=====

output_compressed.pdf

On Tue, May 6, 2025 at 4:36 PM Wendy Vu (ACI) <wendy_vu@asus.com> wrote:

Dear Mr. Fouts,

Thank you for your continued communication and for submitting detailed documentation rega

Your concerns have been formally escalated to our Global Research and Development team for

As outlined in our warranty terms, we require that the products be returned to an ASUS Service

its original factory state and free of any physical damage, we would be happy to consider a buy

In addition, please provide the full and clearly legible serial number (SN) of the affected device,

We would also like to clarify the scope of our support:

- Requests such as a lifetime supply of ASUS products, emergency housing, or similar form
- Additionally, ASUS will not be participating as a co-plaintiff in any litigation. If ASUS's parti

We remain committed to investigating this matter as appropriate, based on the facts and findir

If you may have any additional questions and/or concerns, please do not hesitate to let us know

Thank you!

Best regards,

Wendy Vu | Senior Supervisor of Customer Care

Service Department | Support Section | Corporate Customer Care

Phone: 510-739-3777 ext. 65008 | Email: Wendy_Vu@asus.com

ASUS Computer International | 48720 Kato Road, Fremont, CA 94538



From: John Fouts <icreateupwardspirals@gmail.com>

Sent: Saturday, May 3, 2025 10:29 PM

To: Wendy Vu (ACI) <wendy_vu@asus.com>; asus cc (ACI) <asus_cc@asus.com>

Cc: Jennifer Stover (ACI) <Jennifer_Stover@asus.com>; Wendy Vu (ACI) <wendy_vu@asus.com>;

Subject: [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]2025-05-04 - Subject: URGENT -

External email : Ensure your email is secure before opening links and attachments.

Subject: URGENT – Firmware Compromise Confirmed: Updated Evidence Submission + Escalation Follow-Up

Hi Wendy,

Thank you again for your response. I am continuing to gather and send the materials you requested. Please see tl

- Serial numbers and official purchase receipts for the ASUS TUF Gaming A16 and AX1800 router - AX5400
- Product box photos and identifying labels
- A forensic evidence archive containing ACPI firmware tables (DSDT, SSDT1–23, IVRS, TPM2, VFCT, etc.)
- Boot logs showing Secure Boot bypassed and kernel virtualization activity
- Additional screenshots and data supporting our case of firmware-level and hypervisor compromise

The latest evidence now confirms:

- **Presence of stealth hypervisor behavior in the kernel logs**, including the line:
Booting paravirtualized kernel on bare hardware
- **Injection of Microsoft Hyper-V drivers** into a non-Hyper-V Linux environment
- **Secure Boot disabled** despite BIOS settings indicating otherwise
- **ACPI tables** such as IVRS, TPM2, and VFCT, and up to 23 custom SSDT entries with rogue identifiers (CPI
- **Failure of ASUS firmware security** to protect against virtualization-layer compromise and PCIe bus decey

These facts are verifiable, reproducible, and irrefutable. I expect this to be escalated immediately to your firmware

I am reiterating my original formal demands:

- A **Lifetime Protectional Contract Guarantee** and **Lifetime Supply of uncompromised equipment** for m
- ASUS's participation as a **co-plaintiff in related federal litigation**
- Immediate preservation of logs, internal findings, and supply chain traceability
- A formal **Non-Retaliation Agreement**
- Compensation for the documented damages
- Coordination with federal agencies including **FTC, IC3, CISA, and HIPAA enforcement**

Attachments:

- ASUS_ACPI_evidence_bundle.zip
- ASUS 1800 router + ASUS A16 Tuf Gaming laptop receipts (PDF/JPG) - the AX5400 Receipt for that route
- Terminal logs and screenshots (PDF)
- Cyber_Espionage_Legal_Notice_Meta.pdf
- Gmail - 2025-04-10 URGENT_Cyber Espionage Report & Legal Notice – ADA-Prote
- EXHIBIT-EMERGENCY MEDICAL-NECESSITY-LETTER-DR-JORDAN-VAUGHN.pdf

1. **Immediate relocation and emergency housing**, paid for by ASUS, to ensure the safety of myself and my
2. **Immediate replacement of all compromised ASUS devices**, including the TUF Gaming A16 and AX1800
3. A **lifetime supply of top-tier, secure ASUS computing and networking equipment** for both myself and
4. Ongoing ASUS-based system integrity checks or trusted partner support to ensure continued protection
5. **Immediate filing by ASUS of a federal legal case** in partnership with me, listing ASUS and myself as **co-**
6. **Filing of a formal police report** by ASUS with:
7. Local law enforcement (Jeffersontown Police Department and Louisville Metro Police Department),
8. The Louisville FBI Field Office, local DOJ office
9. And relevant federal cybersecurity agencies (FTC, CISA, IC3, FCC),

to launch a coordinated investigation into the supply chain compromise and resulting harm

10. A **formal Lifetime Protectional Contract Guarantee** for myself and my child
11. A **Formal Non-Retaliation Agreement**
12. **Comprehensive forensic transparency**: ASUS must preserve all related internal firmware records and log
13. Immediate preservation of logs, internal findings, and supply chain traceability
14. Compensation for the documented damages

The evidence now confirms:

- Firmware ACPI tables (DSDT, SSDT1–23, IVRS, TPM2, VFCT, WSMT) have been modified or injected with \
- Boot logs show **paravirtualized kernel activity on bare hardware**
- Secure Boot is disabled despite UEFI settings
- Microsoft Hyper-V kernel modules were **injected without consent**
- Custom ACPI identifiers (CPMACPV7, CPLTFG, GPPS_PME, AMDW0V, etc.) strongly suggest spoofed PCIe b

There is additional evidence as well that I will hold onto at this point in time

This is not theoretical. It is **proven, forensic, and actionable**. These failures trace directly to ASUS hardware and
• [final_evidence_ocr_fixed.pdf](#)

These findings are irrefutable and documented across multiple forensic snapshots. I am operating with every form

Please confirm:

- Receipt of the attachments
- Immediate initiation of the above actions
- Timeline for ASUS's formal response, device replacement, relocation, and legal engagement


This is a life-threatening emergency, and I am copying federal authorities to ensure this matter is recorded and es


Respectfully,

Mr. John R. Fouts, MBA

Plaintiff, Civil Rights Advocate, and Legal Guardian of J.A.F.

 icreateupwardspirals@gmail.com

 502-956-0052 (text only)

 502-996-8246 (HIPAA Compliant)

CC:

 ic3@fbi.gov

 consumer@ftc.gov

 alerts@cisa.gov

On Wed, Apr 30, 2025 at 6:40 PM Wendy Vu (ACI) <wendy_vu@asus.com> wrote:

Dear Mr. Fouts,

Thank you for contacting ASUS and for taking the time to share the serious concerns you've e
take your message seriously, and we are committed to giving your situation the careful atten

At ASUS, we take product security and customer safety with the utmost seriousness. Our dev
We continually assess and improve our hardware and firmware integrity to ensure the protec

To initiate a formal review and escalate your case appropriately, we kindly ask that you provide:

1. Serial numbers of all ASUS devices currently in your possession (e.g., the laptop and board)
2. Receipts or invoices confirming your original purchase of these products,

- **The receipt/invoice will need to display the:**

- company's logo
- date of purchase
- cost
- serial and/or model number of ASUS product
- File types accepted: PDF, JPG, PNG, GIF

- **Unacceptable forms of proof of purchase are:**

- bank statements
- screen shots
- forwarded e-mails
- copy & pasted e-mails
- do not accept files attached as TXT or RTF, DOC

3. Any supporting documentation, including forensic reports, logs, screenshots, or other evidence

We understand that gathering this information may be challenging given your current situation. Our product investigation teams and keep you informed at each stage of the process.

Thank you for your patience and cooperation. We're committed to thoroughly reviewing your case.

Best regards,

Wendy Vu | Senior Supervisor of Customer Care

Service Department | Support Section | Corporate Customer Care

Phone: 510-739-3777 ext. 65008 | Email: Wendy_Vu@asus.com

ASUS Computer International | 48720 Kato Road, Fremont, CA 94538



From: John Fouts <icreateupwardspirals@gmail.com>
Sent: Tuesday, April 29, 2025 8:59 PM
To: Wendy Vu (ACI) <wendy_vu@asus.com>; Jennifer Stover (ACI) <Jennifer_Stover@asus.com>;
Cc: ic3@fbi.gov; consumer@ftc.gov; alerts@cisa.gov
Subject: 2025-04-29 - Subject: URGENT: Formal Demand for Immediate Action, Legal Partner

External email : Ensure your email is secure before opening links and attachments.

Dear ASUS Executive and Legal Teams,

Please find attached my formal demand letter and supporting evidence regarding catastrophic digital and physical

This includes:

- A Lifetime Protectional Contract Guarantee and Lifetime Supply of top-tier equipment for both myself and
- ASUS's active initiation of new federal litigation as a co-plaintiff alongside me
- Police report filing and formal escalation to federal agencies (FTC, CISA, IC3, HIPAA, NHTC)
- Preservation and delivery of logs, chain-of-custody documentation, and internal findings
- A Non-Retaliation Agreement
- Compensation for already-incurred damages, and acknowledgment of ASUS's exposure to punitive damages

This situation has involved not only the confirmed compromise of firmware-level security, stealth hypervisors, and

Due to this breach, my child and I are currently displaced and surviving under severe hardship. Delivery logistics

I request for all communication to be in writing via email.

Contact:

- Email: icreateupwardspirals@gmail.com
- Phone: 502-956-0052 - text only
- Fax: 502-996-8246 - HIPAA compliant

Respectfully,

Mr. John R. Fouts, MBA

Plaintiff, Civil Rights Advocate, and Legal Guardian of J.A.F.

Attachment:

ASUS_Demand_Letter_and_Evidence_John_Fouts_FINAL_JAF_REMEDIES_UPDATED.pdf

=====

This email and any attachments to it contain confidential information and are intended solely for the use of the individual named. Please be advised that any unauthorized disclosure, copying, distribution or any action taken in reliance on the contents of this information may be subject to legal action.

For pricing information, ASUS is only entitled to set a recommendation resale price. All customers are free to set their own prices.

=====



How t



PhoX



2025-



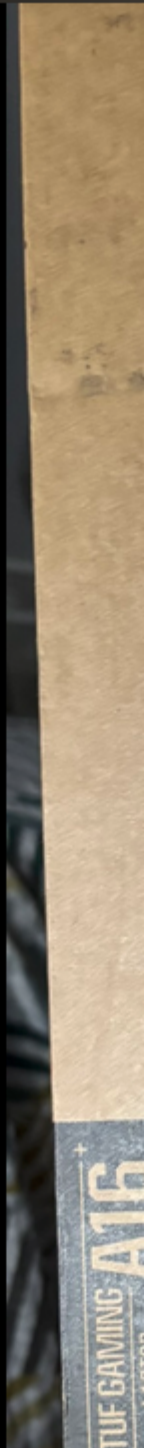
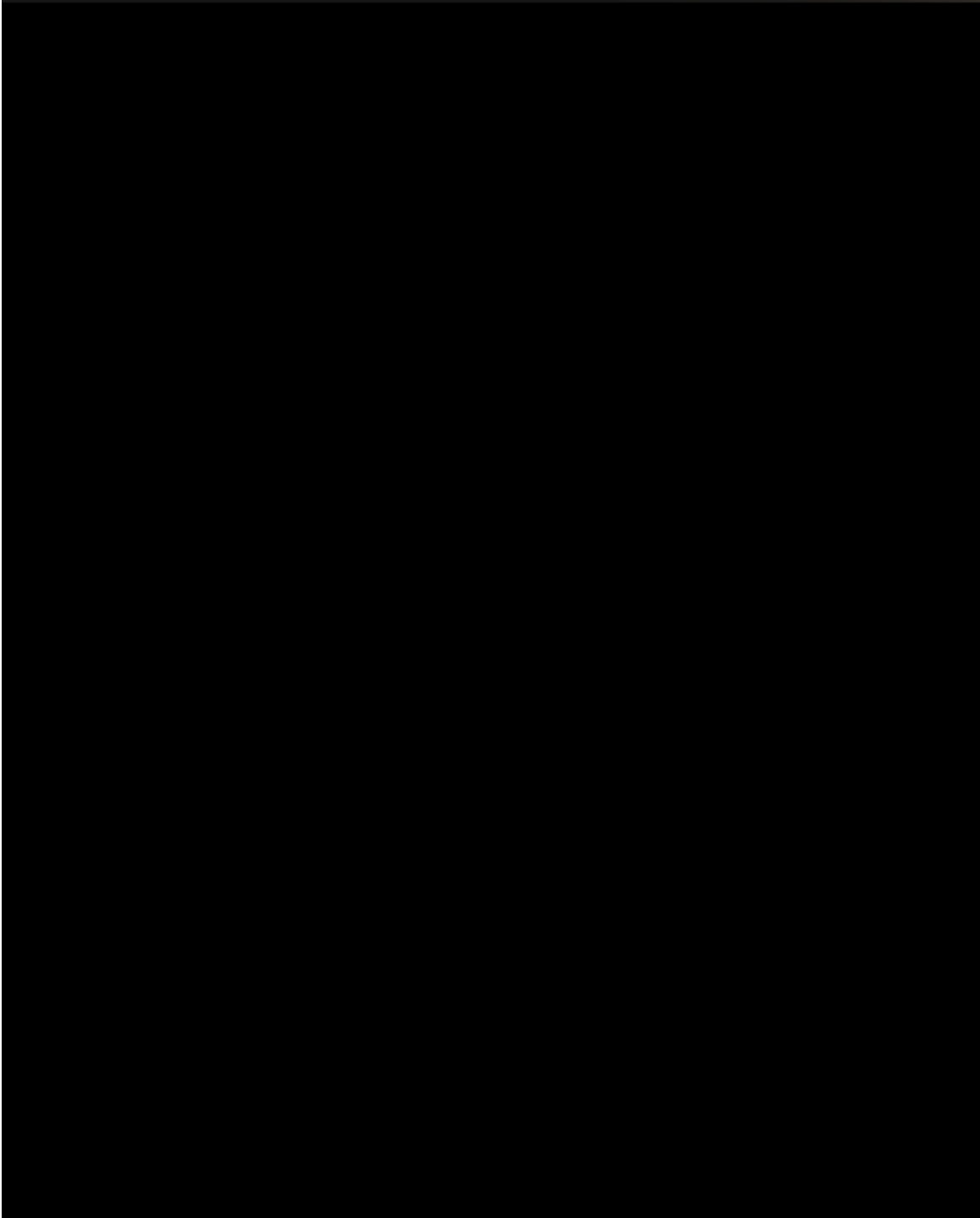
Yosi •

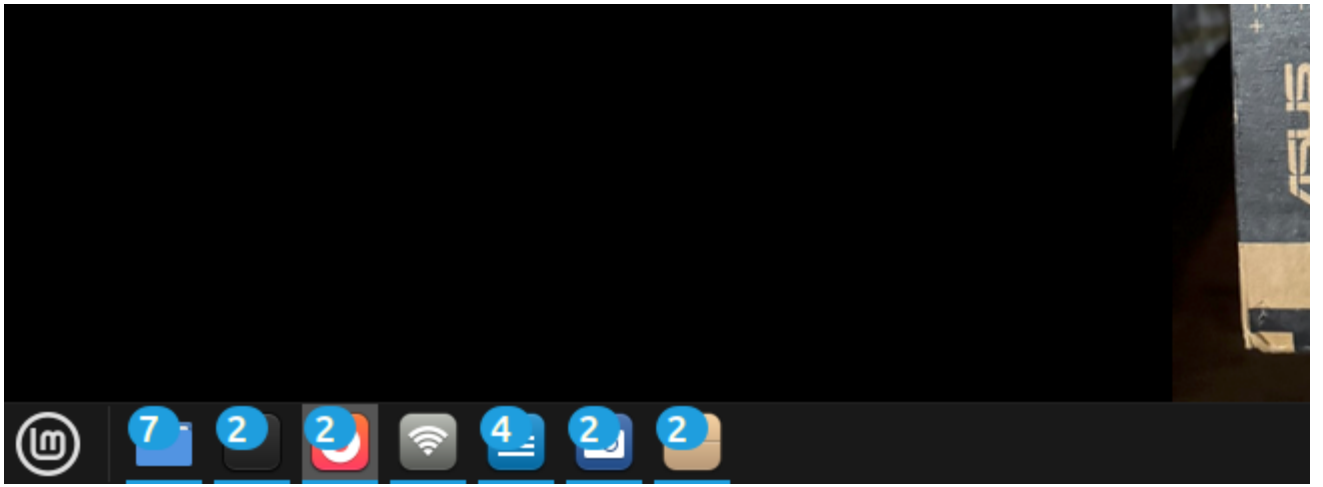


Gem



https://www.icloud







How t



PhoX



2025-



Yosi •



Gem



https://www.icloud



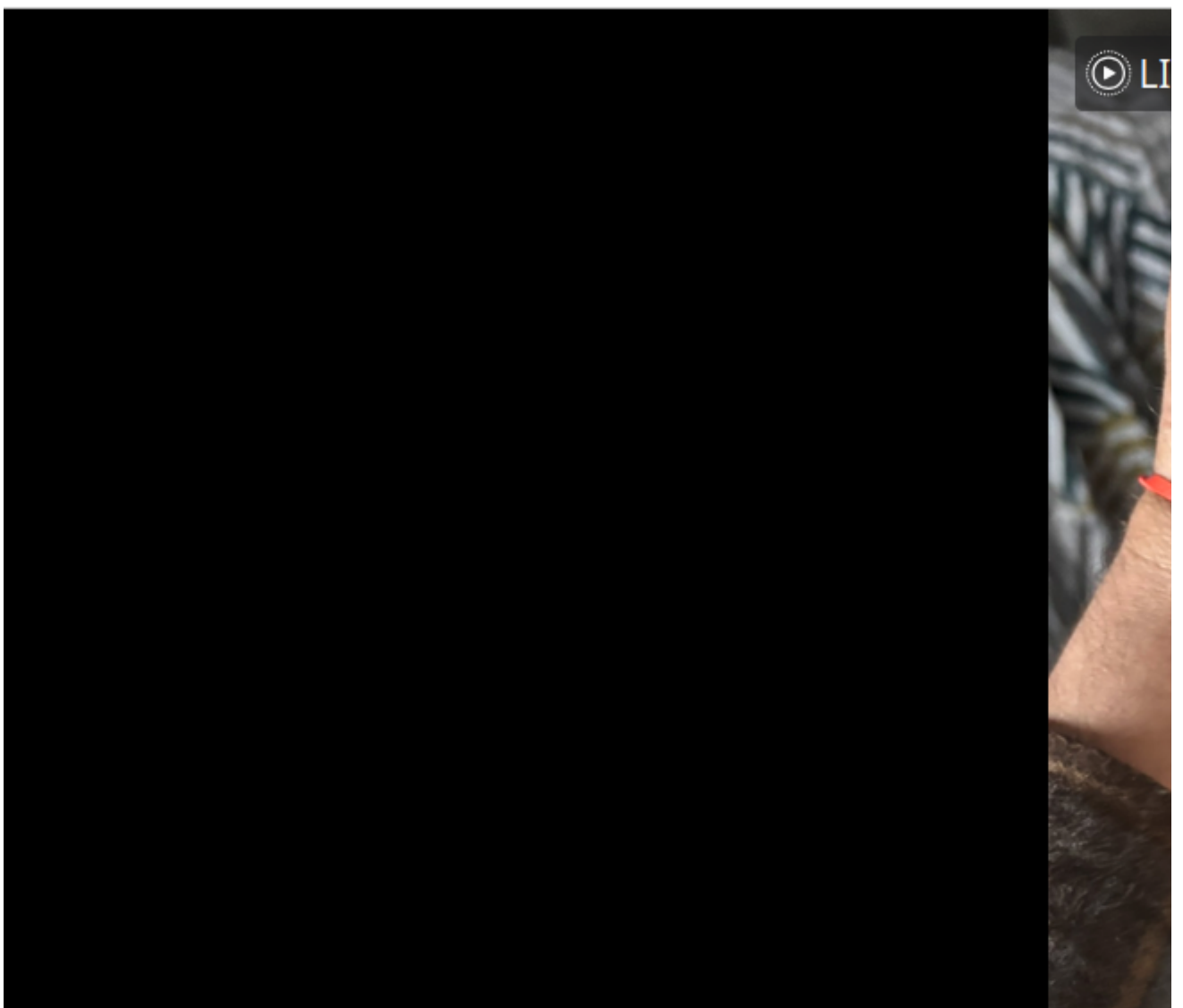
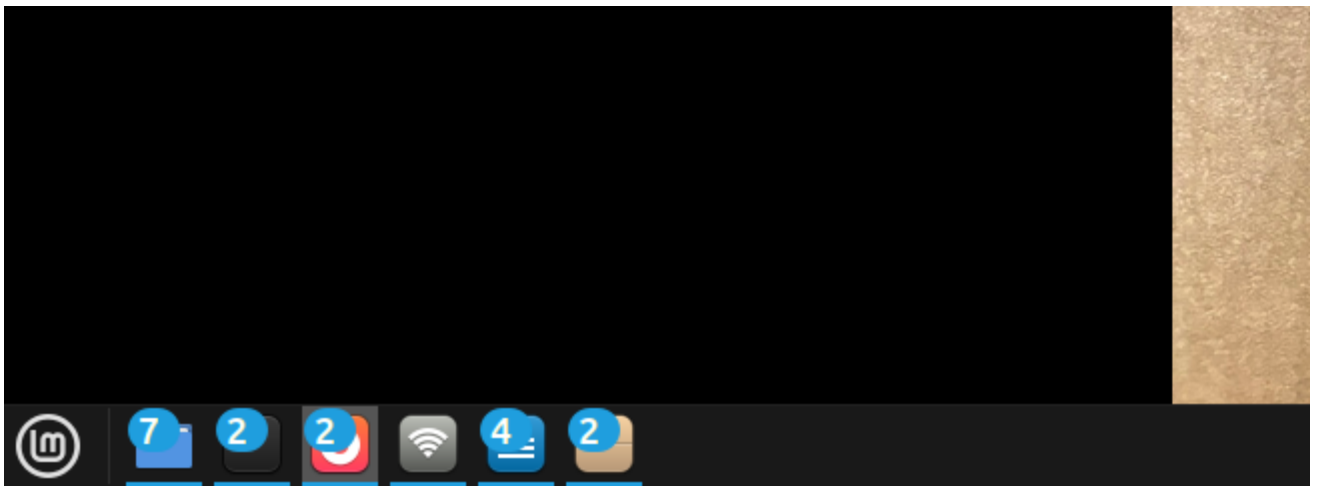
LI

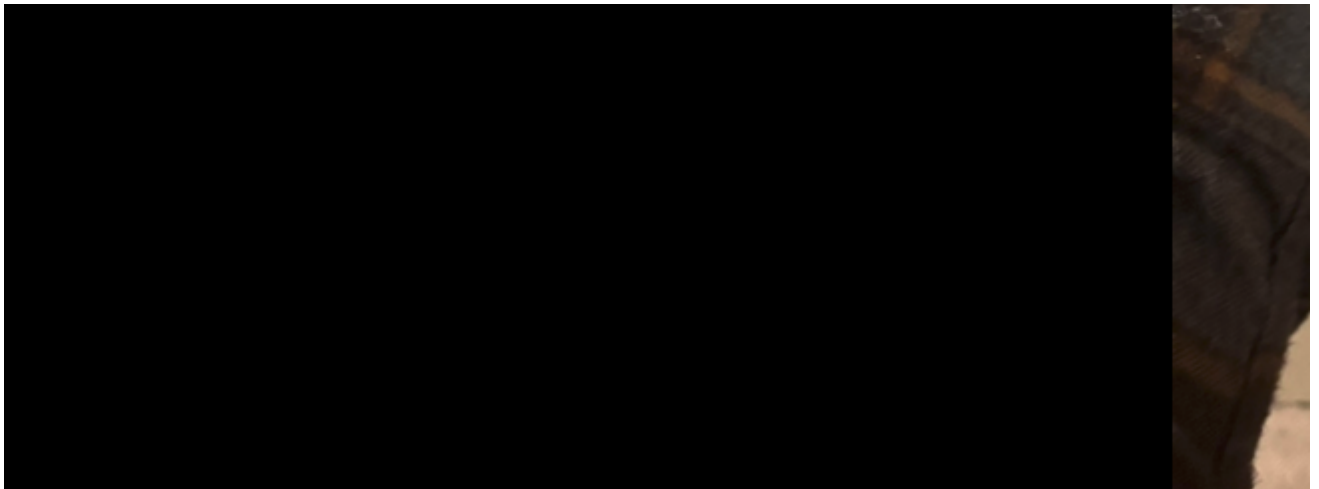
Packin
Thank

To JO
290
JEFF

Produ
ASUS
B 7944
Grey
Targu

If you
at cs4
issue





How to



Phox



2025-



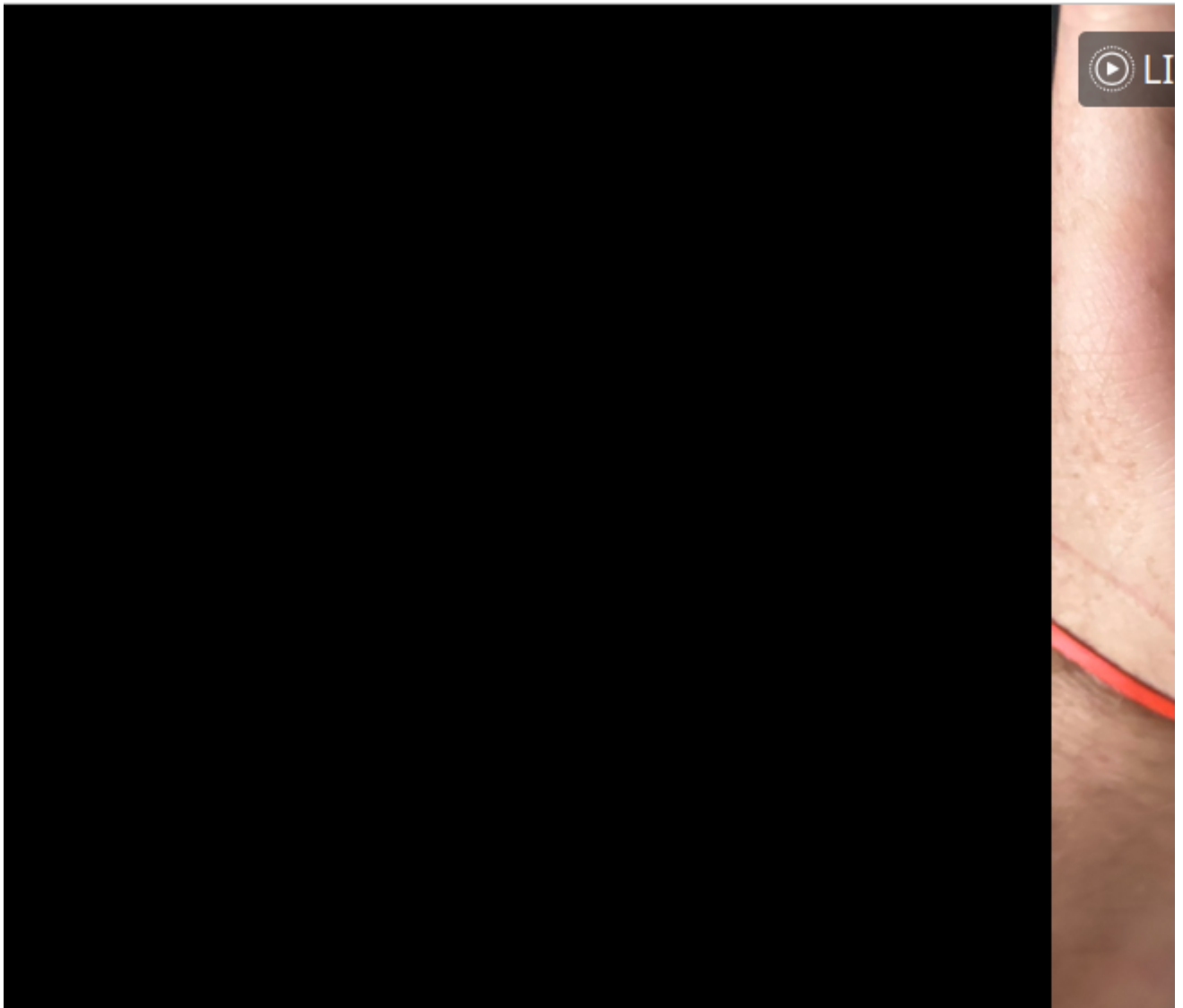
Yosi



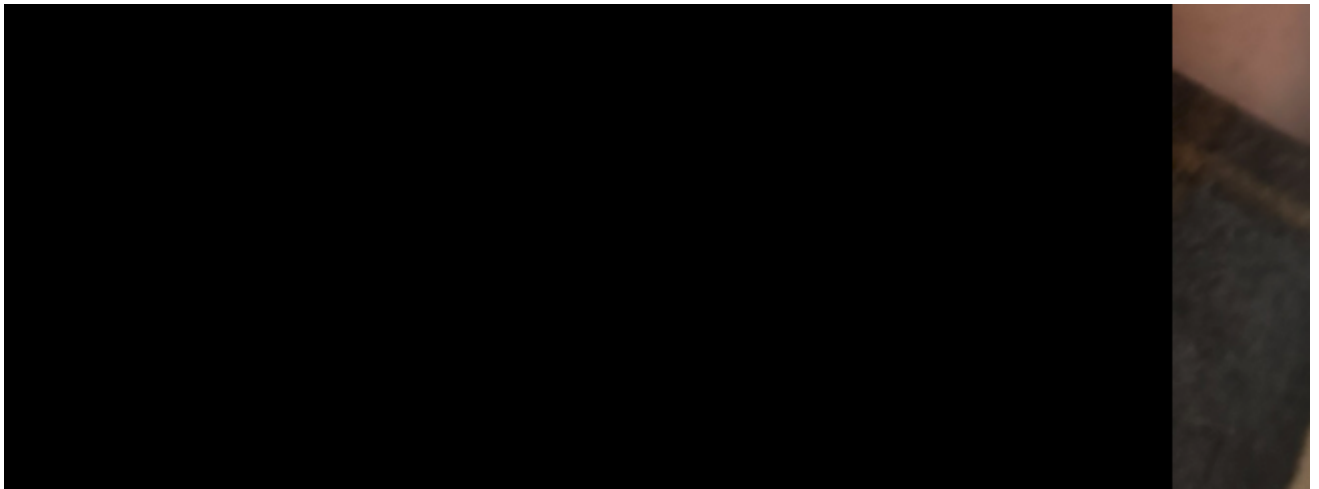
Gem



https://www.icloud



LI



How to



Phox



2025-



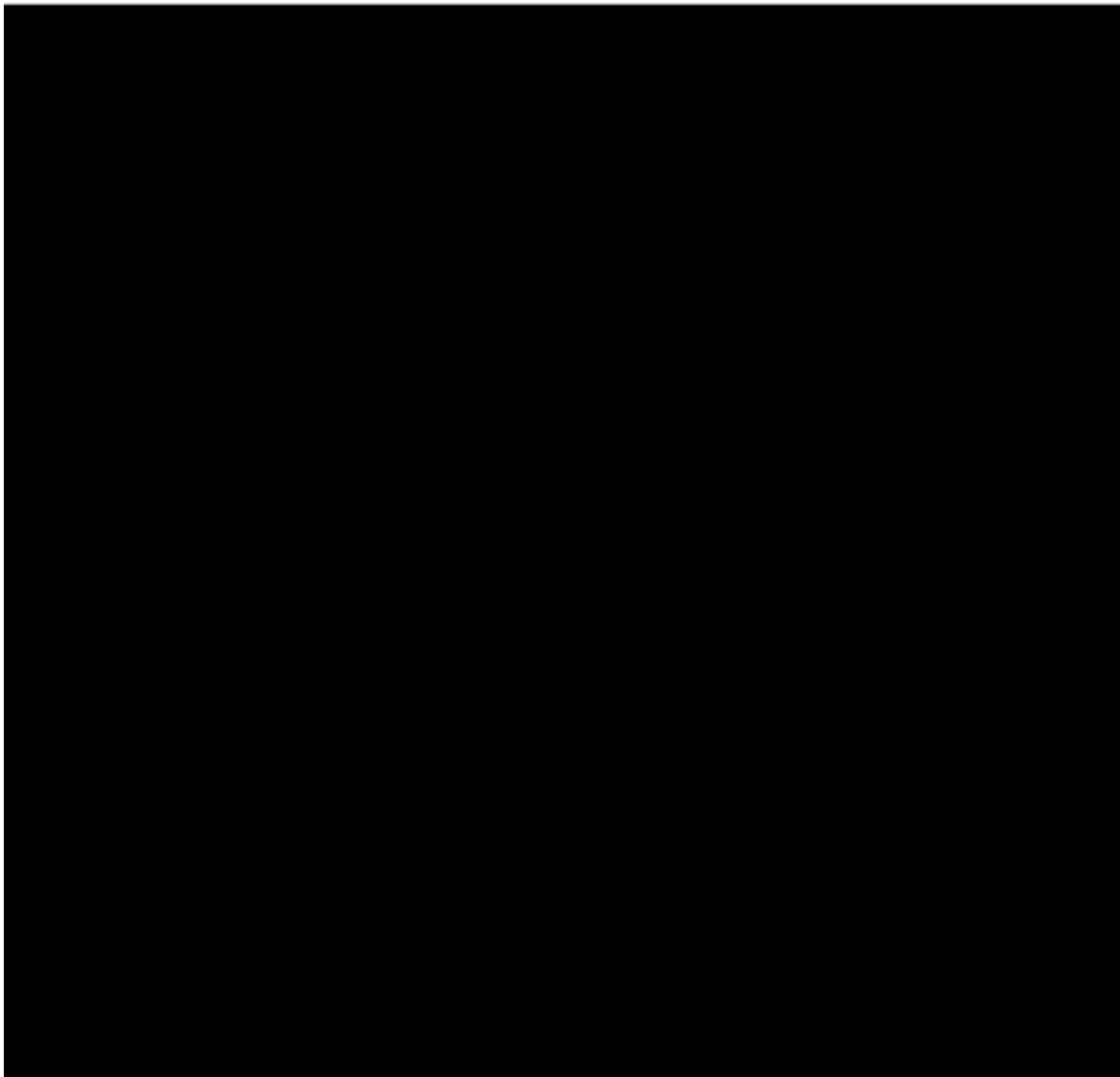
Yosi

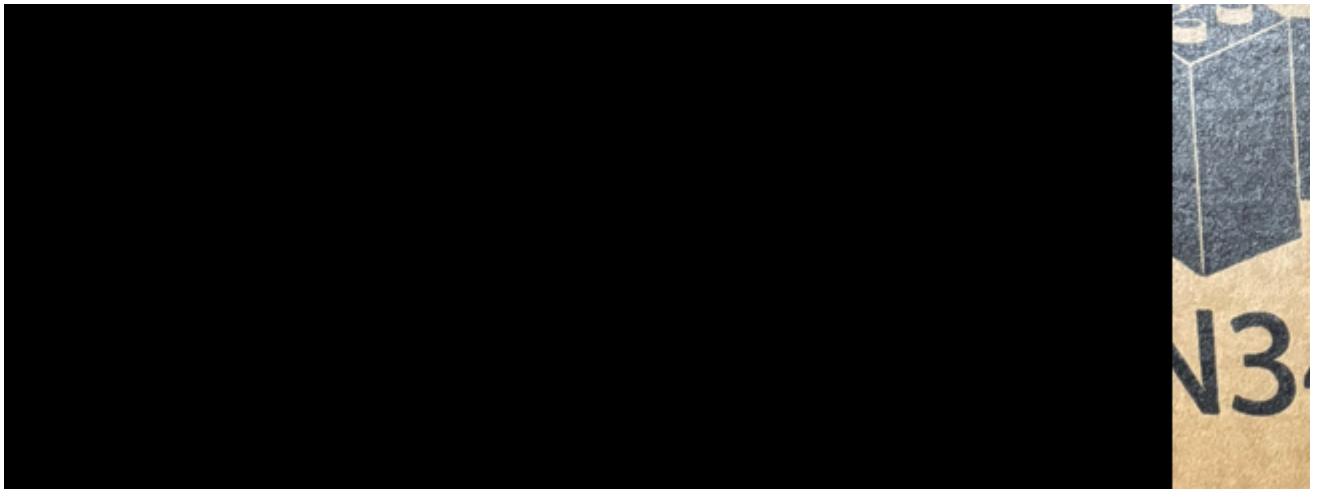


Gem



https://www.icloud





How to



Phox



2025



Yosi



Gem



<https://www.icloud>



LIVE





How to



Phox



2025-



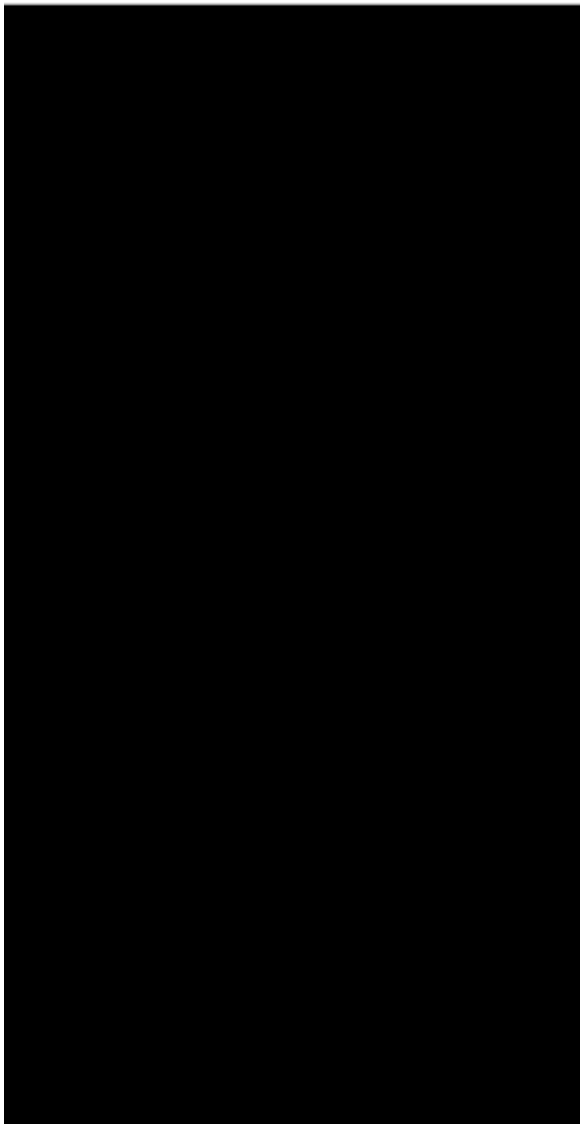
Yosi



Gem



https://www.icloud



LIVE

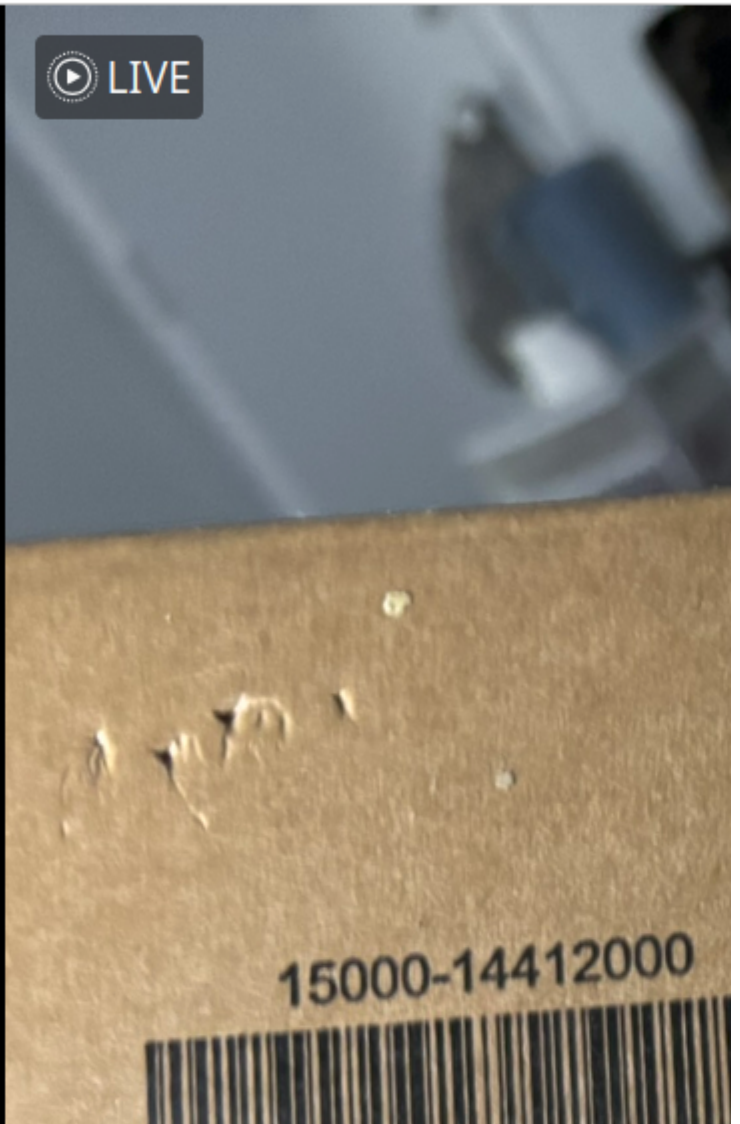




image003.png
1120K



image004.png
1107K

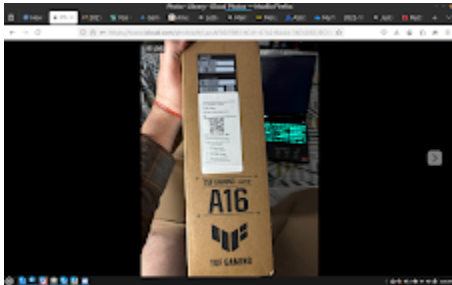


image005.png
1160K

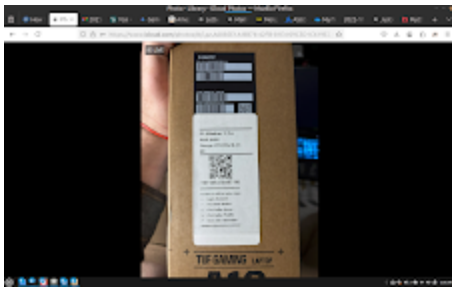


image006.png
1187K



image007.png
1483K

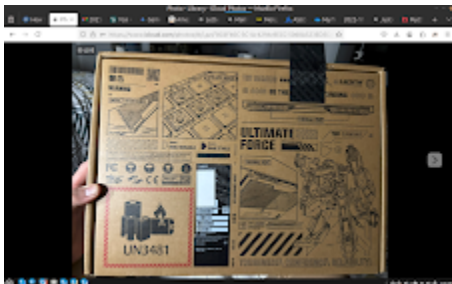


image008.png
2409K

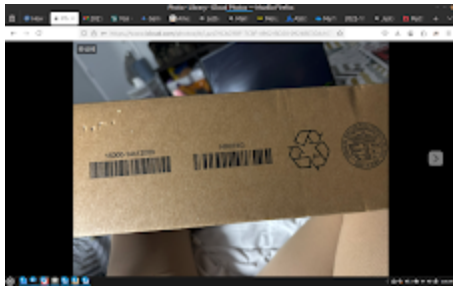


image009.png
1819K